CLAIMS

1. A method (300) for providing conditional access to data (12/52) within a broadband communication system (10), the broadband communication system (10) having a conditional access system (24) responsive to a plurality of subscriber devices (14, 20), the data (52) stored on a recording medium (50) when the recording medium (50) is detachably coupled to a first subscriber device (14) and encrypted using an encryption key (54) associated with the first subscriber device, the method comprising:

based on a request on behalf of a second subscriber device (20) for access to the data (52), arranging (302) for the conditional access system (24) to authenticate the second subscriber device (20); and

after authentication of the second subscriber device (20), arranging (304) for the conditional access system (24) to transfer the encryption key (54) to the second subscriber device (24),

the encryption key (54) usable by the second subscriber device (20) to decrypt the data (52) when the recording medium (50) is detachably coupled to the second subscriber device (20), access to the decrypted data by the second subscriber device (20) restricted in a manner specified by the conditional access system (24).

2. The method according to claim 1, wherein the broadband communication system comprises (10) a cable television system.

3. The method according to claim 2, wherein the cable television system is an interactive two-way system.

4. The method according to claim 2, wherein the cable television system is a one-way system.

5. The method according to claim 2, wherein the first (14) and second (20) subscriber devices comprise set-top boxes.

6. The method according to claim 5, wherein the recording medium (50) is detachably couplable to the first (14) and second (20) subscriber devices via a serial bus implementation, at least in part in compliance with the Institute of Electrical and Electronics Engineers 1394 standard.

7. The method according to claim 6, wherein the recording medium (50) comprises an external personal video recorder.

8. The method according to claim 1, further comprising: prior to arranging for transfer of the encryption key (54) to the second subscriber device (20), arranging for payment of a fee by the second subscriber device (20).

9. The method according to claim 1, wherein the step of arranging for authentication of the second subscriber device (20) comprises arranging for the conditional access system (24) to receive a predetermined identifier from the second subscriber device (20).

10. The method according to claim 1, wherein the data (52) is protected by intellectual property rights of a third party.

11. The method according to claim 10, further comprising:

specifying an access condition associated with the data, the access condition based on the predetermined intellectual property rights.

12. The method according to claim 11, wherein the access condition is specified by the conditional access controller (24).

13. The method according to claim 12, wherein the step of arranging for authentication of the second subscriber device (20) comprises evaluating the access condition.

14. The method according to claim 13, wherein the use of the data (52) by the second subscriber device (20) is restricted in a manner specified by the access condition.

15. The method according to claim 1, wherein the encryption key (54) is created by one of the conditional access controller (24) and the first subscriber device (14).

16. A computer-readable medium (30, 264) encoded with a computer program (34, 222) which, when loaded into a processor (32, 239), implements the method of claim 1.

17. The computer-readable medium (30) according to claim 16, wherein the processor (32) is associated with the conditional access system (24).

18. The computer-readable medium (264) according to claim 16, wherein the processor (239) is associated with the first subscriber device (14).

19. The computer-readable medium according to claim 16, wherein the processor is associated with the second subscriber device (20).

20. An apparatus for providing conditional access to data (12/52) within a broadband communication system (10), the broadband communication system (10) having a conditional access system (24) responsive to a plurality of subscriber devices (14, 20), the data (52) stored on a recording medium (50) when the recording medium (50) is detachably coupled to a first subscriber device (14), and encrypted using an encryption key (54) associated with the first subscriber device (14), the apparatus comprising:

a computer-readable storage medium (30, 264); and

a processor (32, 239) responsive to the computer-readable storage medium (30, 264) and to a computer program (34, 222), the computer program (34, 222), when loaded into the processor (32, 239), operative to:

based on a request on behalf of a second subscriber device (20) for access to the data (52), arrange for the conditional access system (24) to authenticate the second subscriber device (20); and

arrange for the conditional access system (24) to transfer the encryption key (54) to the second subscriber device (20) after authentication of the second subscriber device (20), the encryption key (54) usable by the second subscriber device (20) to decrypt the data when the recording medium (50) is detachably coupled to the second subscriber device (20).

21. A system for providing conditional access to data (12/52) within a broadband communication network (10), the data (52) stored on a recording medium (50) detachably couplable to a plurality of subscriber devices (14, 20), and encrypted using an encryption key (54) associated with a first subscriber device (14), the system comprising:

a network communications interface (42, 259) for forwarding a request for access to the data by a second subscriber device (20); and

an information processing system (44, 253) in communication with the network communications interface (42, 259), for receiving and processing the request forwarded by the network communications interface (42, 259), and, based on the request, performing a method comprising:

arranging for authentication of the second subscriber device (20) by a conditional access system (24) within the broadband communication network (10); and

after authentication of the second subscriber device (20), arranging for the conditional access system (24) to transfer the encryption key (54) to the second subscriber device (20), the encryption key (54) usable by the second subscriber device (20) to decrypt the data when the recording medium (50) is detachably coupled to the second subscriber device (20).

22. The system according to claim 21, wherein the system comprises a headend (22) of a cable television system.

23. The system according to claim 21, wherein the system comprises the second subscriber device (20), and wherein the second subscriber device comprises a cable set-top box.